

## Einführung

Die MICROSENS Switche sind mit einem integrierten Management Agent ausgestattet.

Dieser unterstützt folgende Protokolle:

- **MICROSENS Device Manager** Zentrale Management Plattform,  
2 Benutzerlevel über Passwort
- **SNMP** Bis zu 16 Traps an 8 Empfänger,  
2 Benutzerlevel über Communities
- **Telnet** CLI kompatible Syntax,  
2 Benutzerlevel über Passwort
- **http (web basiert)** Grafisches Interface,  
2 Benutzerlevel über Passwort
- **TFTP** Zentraler Upload von Firmware-Updates
- **SYSLOG** Speicherung von Ereignis-Logfiles auf externem  
SYSLOG Server

Alle Managementinformationen stehen in einem Inband-Management zur Verfügung. Ein spezieller Anschluss ist nicht notwendig, somit bleiben alle Ports für den Anschluss von Endgeräten frei.

## Basic Features

- Integrierter 32 bit Hochleistungsprozessor
- Firmware update über TFTP upload oder MICROSENS Device Manager V3.x
- IP Adresse fest oder dynamisch über DHCP
- Permanente Konfigurationsspeicherung im Flash Memory
- "Reset to factory default"-Konfiguration mittels Taster, Trappenerzeugung
- Zugriffskontrolle durch Access Control List (ACL), max. 16 Einträge

## Port Control

- **Aktivierung/ Deaktivierung pro Port**
- **Auto-Negotiation auf den TX-Ports**
  - Automatische Erkennung der Übertragungsgeschwindigkeit und des Duplex-Modus
  - Manuelle Einstellung der Geschwindigkeit und des Duplex-Modus
- **Auto-Crossover auf den TX-Ports**
  - Automatische Erkennung des Kabeltyps
  - Manuelle Einstellung der PIN-Belegung (MDI [1:1 oder MDI-X [gekreuzt])
- **Netzwerkschleifen Erkennung**
  - Schutz gegen versehentliches oder mutwilliges verbinden zweier Netzwerkports durch die Unterdrückung von „Non-unicast-traffic“
- **Rapid Spanning Tree (RSTP, STP)**
  - Erkennung redundanter Netzwerkpfade bzw. Vermaschungen
- **Traffic Shaping**
  - Bandbreitenlimitierung pro Port
  - Unabhängige Einstellung von Empfangs- und Sendegeschwindigkeit
  - VoIP Bandbreitenlimitierung zur Vermeidung des Missbrauchs von dedizierten VoIP-Ports
- **Remote Fault (LWL Port)**
  - Konfigurierbare „Far End Fault Indication“

## Portbasierende Netzwerksicherheit

- IEEE Std. 802.1x Nutzer Authentifizierung gegen RADIUS Server
  - Authentifizierung mit Nutzernamen/Passwort gegen RADIUS Server
  - Redundanter RADIUS Server konfigurierbar
- Multi-User Authentifizierung pro Port
  - Pro Port können bis zu 4 Nutzer unabhängig voneinander angemeldet werden
  - Jeder Nutzer wird durch seine IP-/MAC Adresse identifiziert
- VoIP Security
  - VoIP Telefone und PC's können unabhängig auf dem gleichen Port authentifiziert werden
- MAC Adressen Authentifizierung gegen RADIUS Server
  - Nutzer MAC Adressen Authentifizierung gegen RADIUS Server
  - Integration von Nicht-802.1x-fähigen Endgeräten
- MAC Adressen Limitierung pro Port (MAC-Locking)
  - Zugriffskontrolle anhand der MAC Adresse
  - 1 bis 4 Nutzer mit definierten MAC Adressen zugelassen
  - die ersten 4 MAC Adressen selbst lernend
- IEEE Std. 802.1x transparent
  - 802.1x EAP Protokoll wird vom Switch durchgereicht
  - Authentifizierungs-Handling durch zentralen Switch
- MAC-Address Notification
  - Protokollierung von veränderten angeschlossenen MAC-Adressen an den Switch Ports

Portbasierende Netzwerksicherheit nach dem Bundesamt für Sicherheit in der Informationstechnik

Maßnahmenkatalog M 4.206 Sicherung von Switch-Ports:

- MAC-Address Notification
- MAC-Locking
- IEEE Std. 802.1x



## Virtual LAN (VLANs)

- Bis zu 16 VLAN IDs aus dem Wertebereich 1-4095
- Individuelle VLAN ID für den internen Management Port
- Individuelle Konfiguration der Default VLAN ID / Priority pro Port

## Port VLAN Modes gemäß IEEE Standard 802.1Q

- **Access**  
Ausgehende Pakete sind nicht getagged, eingehende Pakete sind mit der Default ID / Priority getagged
- **Trunk**  
Alle Pakete sind getagged, ausgehende und eingehende VLAN Tags bleiben unverändert
- **Hybrid**  
Sowohl Endgeräte mit als auch ohne VLAN Tag können angeschlossen werden

## VoIP Unterstützung im Hybrid Modus

VoIP Telefone mit Priority Tag und PC ohne Priority Tag können an einem Port angeschlossen werden.

## Quality Of Service

### Triple Play

- Unabhängige Verkehrsklassen für Video, Sprache, Daten und Management
- 4 unabhängige Hardware-Queues pro Port
- Konfigurierbare Priorisierungsmechanismen
  - Strikte Priorisierung (Höchste Priorität immer zu erst)
  - Weighted fair queuing (8-4-2-1)
- Traffic Classification
  - Layer 3
    - IPv4 DiffServ/IPv6 Traffic Class
    - Individuelle Konfiguration für jeden Code Point / Traffic Class
  - Layer 2
    - VLAN priority tag
    - Mapping on Queues gemäß IEEE Standard 802.1D
  - Layer 1
    - Hardware Priority, pro Port konfigurierbar
- VoIP Priority Support  
Unabhängigkeit vom Telefonhersteller durch Layer2 und Layer3 Klassifikation

## Power over Ethernet (Hardware-Option)

### Volle Implementierung des IEEE 802.3af Standard

- Unterstützung aller Power Klassen (class 0..4)
- Max. 15,4 Watt bei 48 Volt gemäß Standard
- Detaillierte PoE Status Anzeige
  - Ermittelte PD (Powered Device) Klasse pro Port
  - Aktuell aufgenommen Leistung pro Port
- Volle galvanische Trennung zwischen der PoE-Spannung und der Switch-Elektronik gemäß Standard
- Zum Schutz der Endgeräte wird die PoE-Spannung erst nach Erkennung einer gültigen PoE-Signatur aktiviert
- Automatische Stromabschaltung bei Überstrom und Über-/Unterspannung
- Spezieller „Forced-Power-Mode“ für ältere nicht-802.1x-konforme Endgeräte, das Leistungsaufnahmelimit wird überwacht.

### Erweitertes Power Management

- Für den Gebrauch von Stromversorgungen mit limitierter Leistung
- Für die Speisung mehrerer Switches mit einer einzelnen Stromversorgung
  - **Power-Class Limit pro Port**  
Endgeräte mit höherer Power-Class werden verworfen
  - **Power Limit pro Port**  
Engeräte mit höherer Leistungsaufnahme werden verworfen
  - **Power Limit pro Switch**  
Bei Überschreitung des gesetzten Power-Limits werden Port in vorab bestimmter Reihenfolge deaktiviert
  - **VoIP Security**  
Die Versorgung des Port 1 bleibt für Notrufe immer aktiv

## Netzwerk Diagnose

### Statistic Counters

- 10 RMON Zähler pro Port (Traffic und Fehler)
- Für detailliertes Traffic Monitoring und zur Fehler-Eingrenzung
- zurücksetzbar durch das Management

### Port Monitoring

- Portspiegelung konfigurierbar
- Für detaillierte Traffic-Analyse, Netzwerk-Sniffer, Intrusion Detection
- Quell- und Zielport konfigurierbar
- Richtung (TX/RX) konfigurierbar

## Unterstützte Standards

### IEEE Bridging

802.1d	MAC Bridging
802.1p	Priority tagging
802.1q	Virtual Bridged Local Area Network (VLAN)
802.1x	Port-Based Network Access Control (Authentication)
802.1D	Rapid Spanning Tree

### IEEE Medium Access und Physical Layer

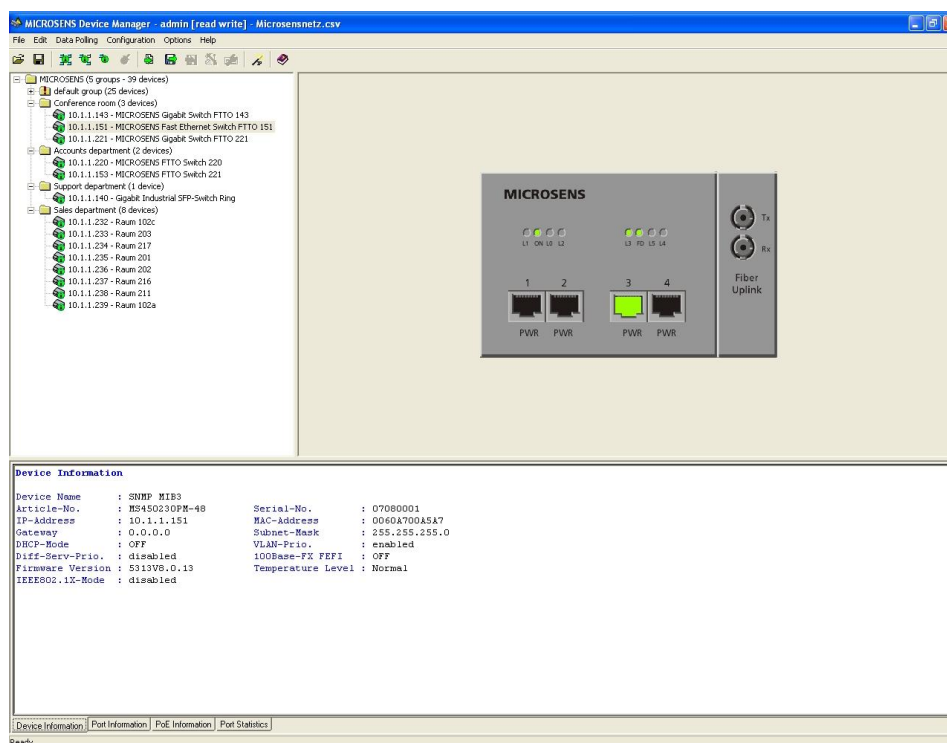
802.3	Ethernet
802.3i	10Base-T
802.3u	Fast Ethernet
802.3ab	Gigabit Ethernet
802.3x	Full Duplex Operation (Flow Control)
802.3ac	Frame Extension for VLAN Tagging on 802.3
802.3af	Power-over-Ethernet

## Management Plattformen

### MICROSENS Device Manager

Mit Hilfe des PC-basierenden Managementtools können sämtliche Funktionen der Installations-Switches konfiguriert werden. Statusinformation können ebenso abgerufen werden wie Herstellerinformationen zum Gerät (Abb. 1).

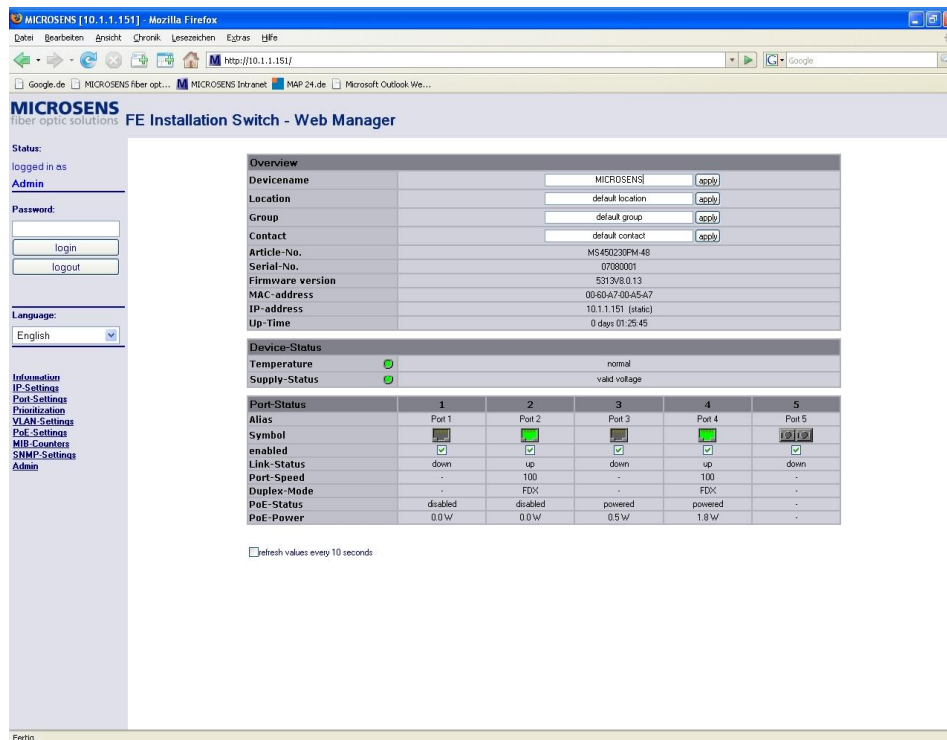
Mit dieser Applikation erfolgt u. a. auch die erstmalige Zuweisung der IP-Einstellungen (IP-Adresse, Gateway und Subnet).



**Abb. 1: MICROSENS Device Manager**

## Web Management

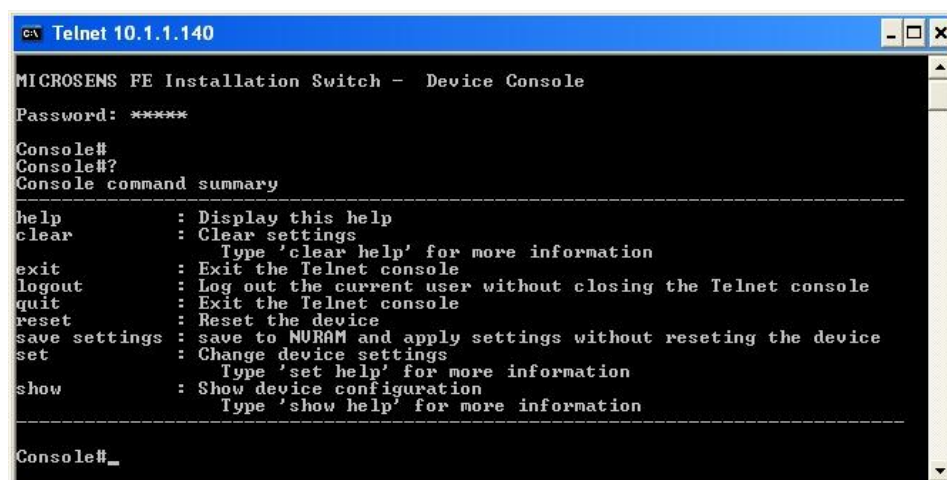
Die Standard-Firmware bietet neben dem MICROSENS Device Manager auch den Zugriff über ein grafisches HTTP-Interface (Abb. 2) zur Visualisierung bzw. Einstellung. Der Zugriff ist mit Hilfe eines standardisierten Internet-Browsers möglich.



**Abb. 2: WEB basiertes Management (http)**

## Telnet Management

Weiterhin besteht die Möglichkeit über die Telnet-Konsole (Abb. 3) alle möglichen Einstellungen mit CLI kompatiblen Syntaxbefehlen durchzuführen.



**Abb. 3: Telnet**

### SNMP (Simple Network Management Protocol)

Mit der Implementierung der MICROSENS Private MIB ist es möglich sämtliche Einstellung und Statusabfragen mit Hilfe einer herstellerunabhängigen SNMP-Management Plattform (Abb. 4) durchzuführen. Status Ereignisse können mit bis zu 16 unterschiedlichen Traps angezeigt werden.

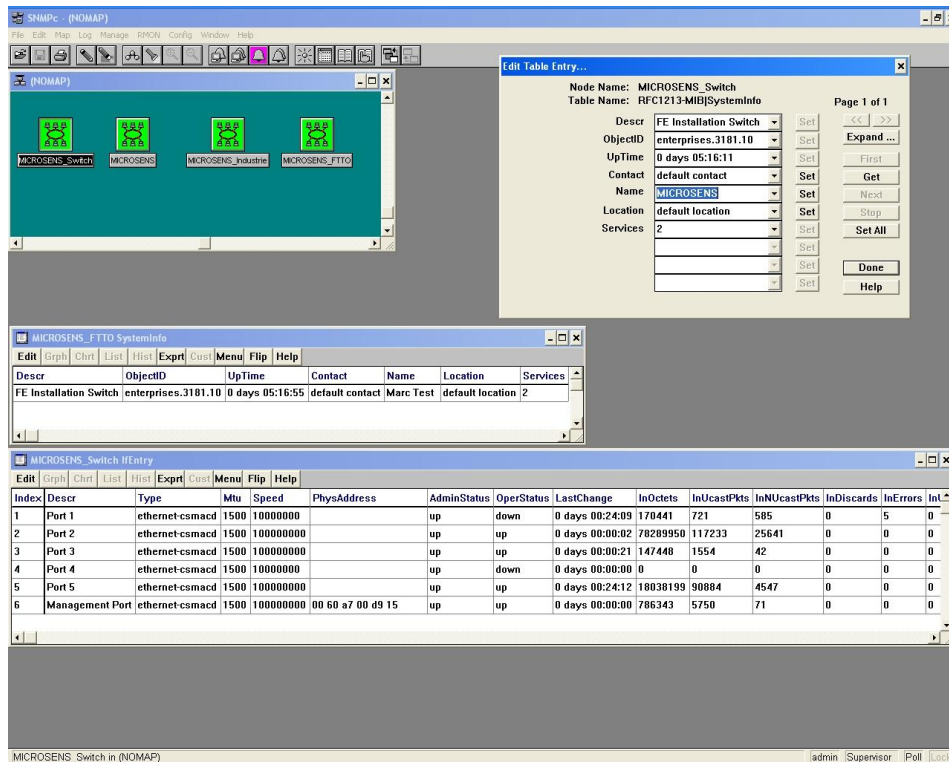


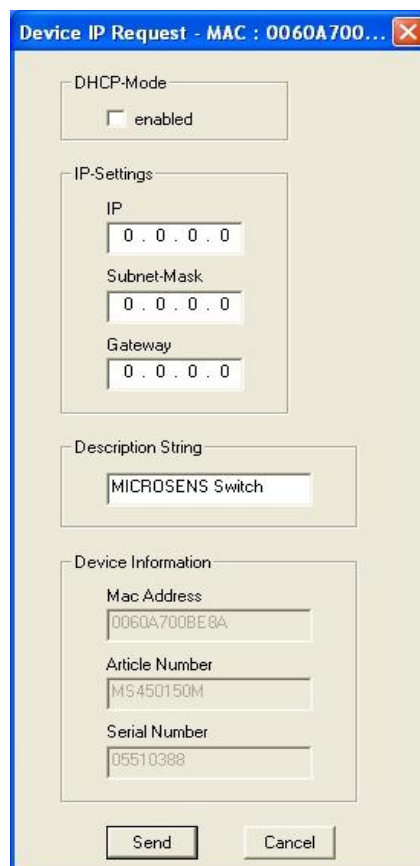
Abb. 4: SNMP Management

## Managementkonfiguration

Die Konfiguration für Management und Gerät werden unterschieden. Während die Konfiguration für das Gerät mit Hilfe des Factory-Resets zurückgesetzt werden kann, bleibt die Konfiguration des Agents stets erhalten. Auch das Einspielen von Firmware-Updates hat keine Auswirkungen auf die Konfiguration des Managements.

Vor der ersten Inbetriebnahme des Managements müssen TCP/IP-Einstellungen für den Agent im Switch vorgenommen werden. Für die erstmalige Zuweisung wird am Gerät durch längeres Auslösen (ca. 5 Sek.) der Reset-Taste ein IP-Request (Abb. 5: IP-Request) ausgelöst.

Für den Empfang über das Netzwerk müssen sich Gerät und PC mit der Device Manager Software im gleichen Segment befinden. Zur Auswahl stehen eine automatische Zuweisung per DHCP-Dienst oder eine manuelle Vergabe.



**Abb. 5: IP-Request**

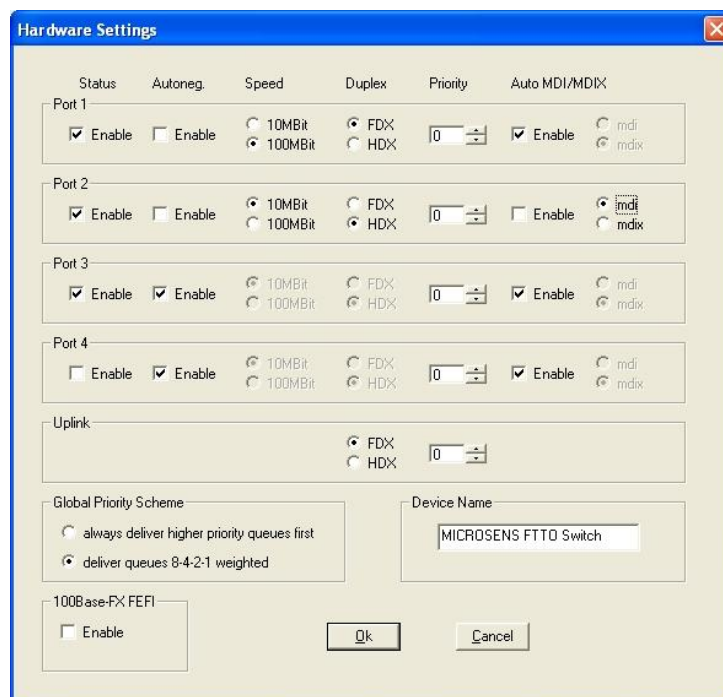
Manuell zugewiesene TCP/IP-Einstellungen können mit der Device Manager Software jederzeit über das Menü „Configuration“ / „Apply IP to current“ geändert werden.

## Konfiguration Hardware

Alle Ports des Switches können individuell konfiguriert werden (Abb. 6a/b).

Folgende Einstellungen sind möglich:

- Port enable/ disable
- Port Auto Negotiation oder manuelle Einstellung Datenrate (10/100Mbit) und Duplex-Modus (voll/halb)
- Hardware Priorität des Ports in 4 Stufen
- Auto Crossover oder manuelle Einstellung Port mit MDI oder MDI-X Belegung
- Uplink Konfiguration Full/ Halb Duplex
- 100Base-FX FEFI: Far-End-Fault-Identification, der Glasfaser-Uplink erzeugt nur ein Link-Signal, wenn auch ein gültiges Link-Signal empfangen wird
- Global Priority Scheme: Gewichtung der vier Warteschlangen für die Quality-of-Service (QoS)
- Device Name: dient zur Geräteidentifizierung, ist identisch mit dem System-Name (SNMP)



**Abb. 6a: Device Manager Hardware Settings**

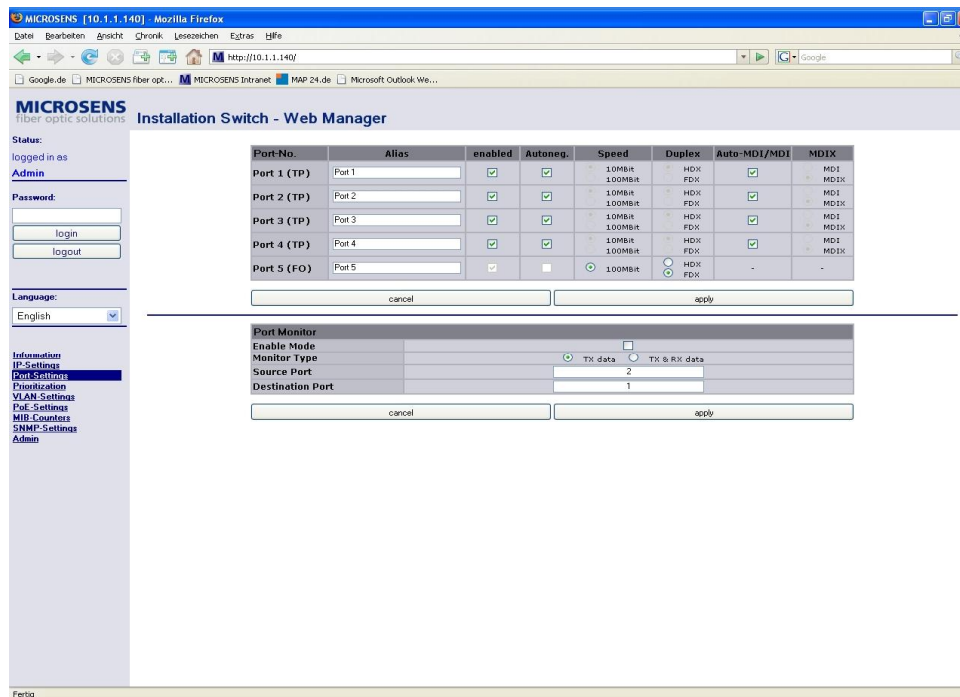


Abb. 6b: WEB Management Hardware Settings

## Daten-Priorisierung

Für die Datenpriorisierung unterscheidet der Switch in vier Warteschlangen (Hardware-Queues 0 bis 3). Anhand von Einstellungen der einzelnen Priorisierungsmechanismen für die Layer 1-3 entscheidet der Switch, welches Datenpaket einer entsprechenden Warteschlange zugeordnet wird.

Warteschlange 0 hat die niedrigste, Warteschlange 3 die höchste Priorität. Im Abschnitt Hardware Settings (s. Abb. 6a/b, Global Priority Scheme) wird festgelegt, in welchem Verhältnis diese Warteschlangen bedient werden sollen.

Die Warteschlangen werden entsprechend der Priorität abgearbeitet (3 -> 2 -> 1 -> 0). Zusätzlich kann eine Gewichtung der Warteschlangen aktiviert werden. Bei der gewichteten Abarbeitung werden zuerst 8 Datenpakete aus der Warteschlange 3 (gemäß höchster Priorität), dann 4 Datenpakete aus Warteschlange 2, dann 2 Datenpakete aus Warteschlange 1 und 1 Datenpaket aus der Warteschlange 0 abgearbeitet.

Folgende Priorisierungsmechanismen werden unterstützt

- **Layer 1:**

Diese Option wird mit der Anschluss-Konfiguration festgelegt. Hier erfolgt eine feste Priorisierung des Anschlusses. Die Konfiguration erfolgt durch die „Standard settings“ (s. Abb. 6a/b). In der Spalte „Priority“ wird direkt die Nummer der Warteschlange (0-3) für den Anschluss eingetragen.

- **Layer 2:**

Auf der Basis von Layer 2 erfolgt die Priorisierung durch das Auswerten des VLAN-Tags (VLAN gemäß IEEE 802.1q). Die Priorität wird durch 3 Bits (entspricht 8 Prioritätsstufen 0-7) gewertet, wobei 7 der höchsten Stufe entspricht. Die Zuordnung der 8 Prioritätsstufen zu den 4 Warteschlangen gemäß IEEE 802.1q wird mit den Settings für VLAN-Priorisierung aktiviert (s. Abb. 7a/b).

- **Layer 3:**

Die Methode Differentiated Services (DiffServ) setzt auf Layer 3 auf. Hierzu werden die ersten 6 Bits von Type of Service Feld (ToS) im IP-Header benutzt. Damit sind 64 Prioritätsklassen möglich. Die Zuweisung der einzelnen Prioritätsklasse auf die jeweilige Warteschlange erfolgt per Konfiguration „DiffServ/Traffic Class Settings“. Diese Funktion ist kompatibel zu IPv6.

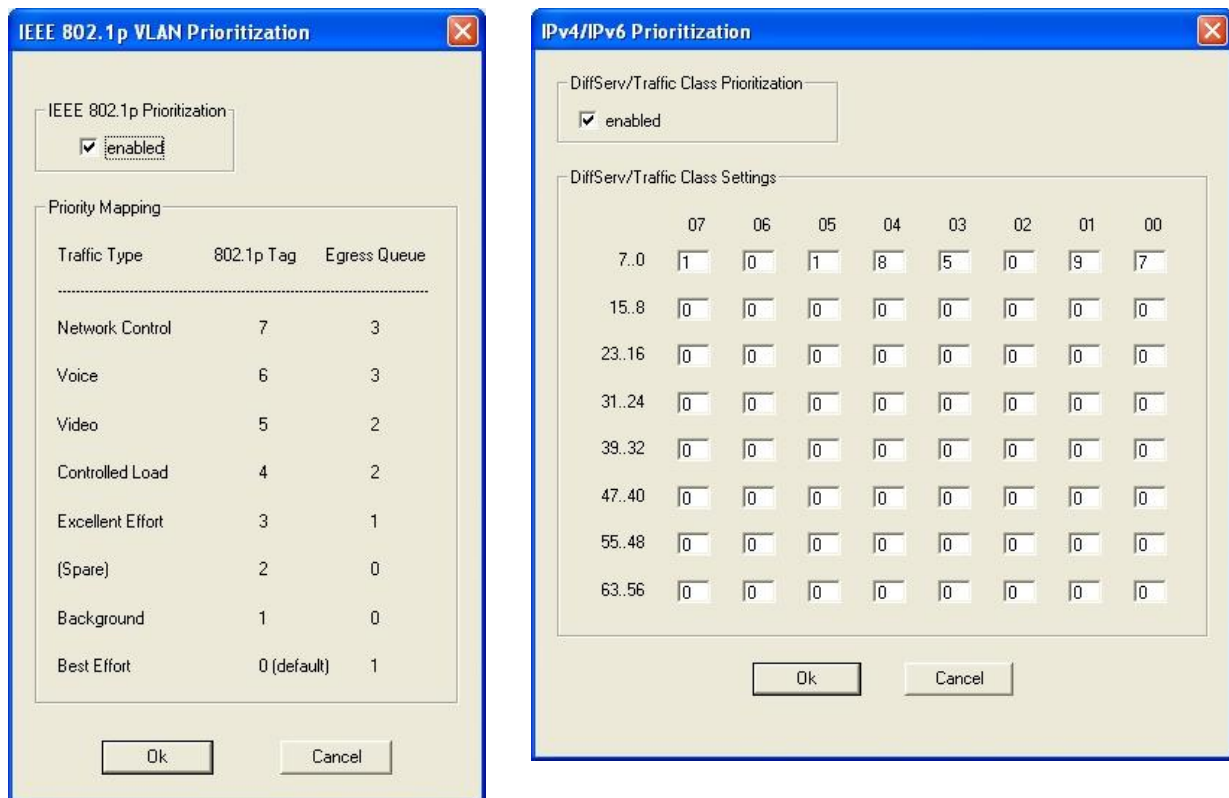
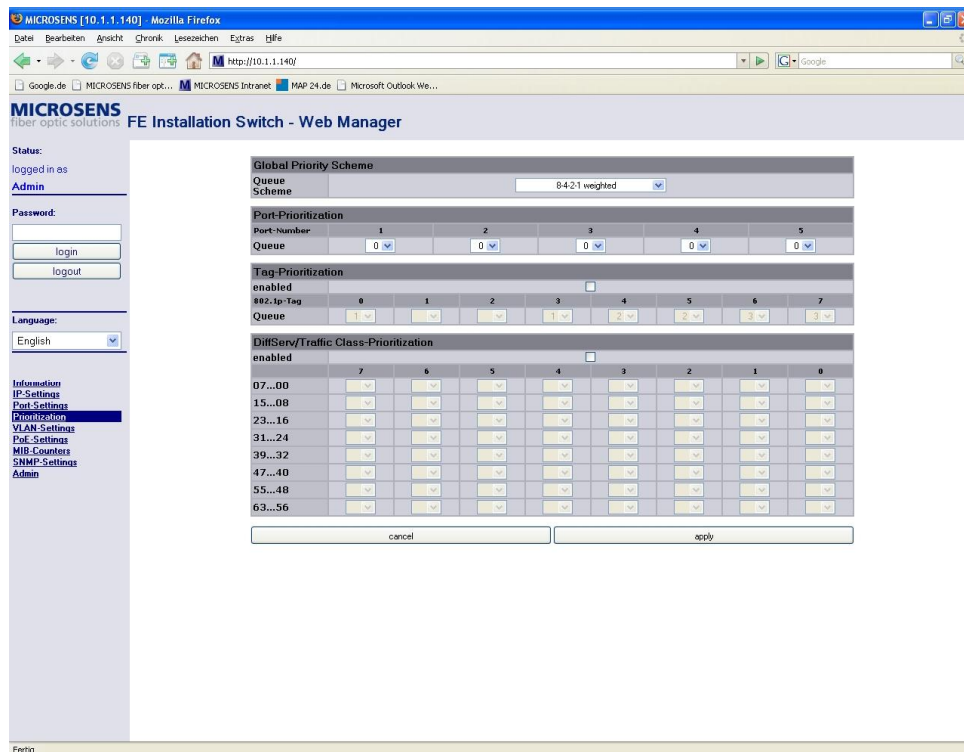


Abb. 7a: Device Manager Priorisierung per Layer 2 bzw. Layer3



**Abb. 7b: Priorisierung per Layer 2 bzw. Layer3**

Die Priorisierungsmechanismen der Layer 1-3 können parallel genutzt werden, wobei der höhere Layer die entsprechende Priorität vorgibt. Somit wird bei einem Datenpaket mit VLAN-Tag die Priorität entsprechend ausgewertet, unabhängig davon welcher Warteschlange der Anschluss (Priorisierung durch Layer 1) zugeordnet wurde.

## VLAN-Einstellungen

Durch die Verwendung von VLANs ist es möglich, lokale Netzwerke unabhängig von der physikalischen Topologie logisch zu segmentieren.

Um sicherzustellen, zu welchem VLAN ein Datenpaket gehört, werden die Datenpakete um das VLAN-Tag (4 Bytes) erweitert. Dieses VLAN-Tag beinhaltet eine in der Norm IEEE 802.1q festgelegte VID (= Virtuelle ID).

- **Access:**

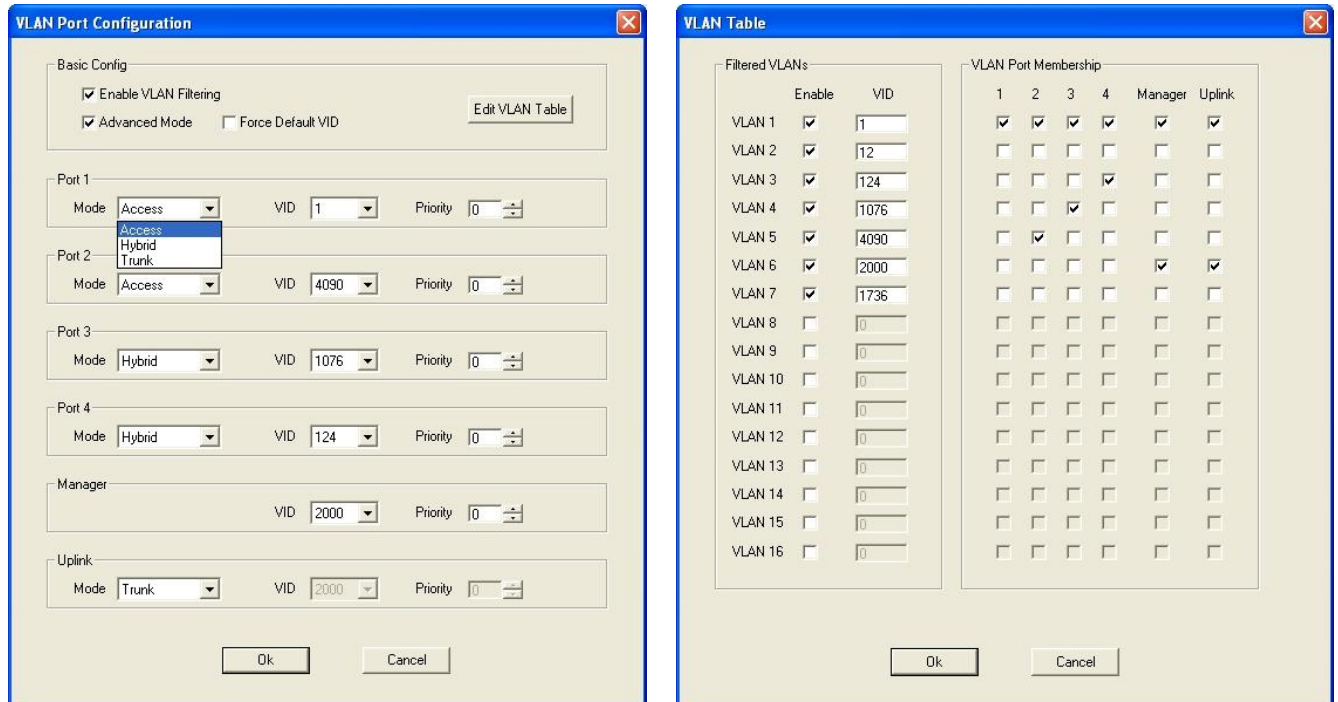
Der Switch fügt den ankommenden Datenpaketen ein VLAN-Tag ein. Der Inhalt (VID und Priorisierung) kann als Port VLAN konfiguriert werden. Besitzen ankommende Datenpakete bereits ein VLAN-Tag, werden diese unverändert weitergeleitet.

- **Trunking:**

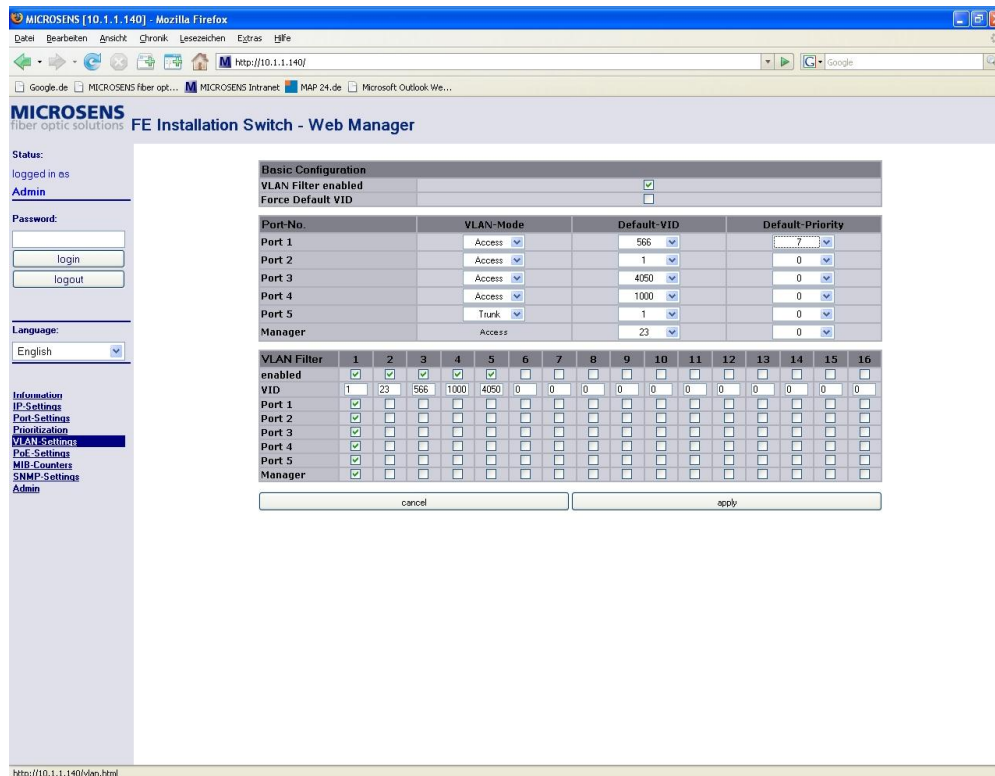
Die über den Port fließenden Datenpakete werden nicht verändert (keine Änderung der VID). Die Filterung erfolgt gemäß den in der VLAN Tabelle frei gegebenen VLANs. Dem Switch können bis zu 16 VLANs aus den 4096 möglichen vergeben werden.

- **Hybrid:**

Ein kombinierter Einsatz von Endgeräten mit VLAN- bzw. ohne VLAN-Unterstützung ist möglich (PC ohne VLAN an Kaskade-Port eines IP-Telefons). In diesem Fall werden nur in Datenpaketen ohne VLAN-Tag ein Tag mit einer vorgegebenen VID eingefügt. Beim Verlassen der Datenpakete aus dem Netzwerk werden nur die VLAN-Tags der vorgegebenen VID wieder entfernt.



**Abb. 8a: VLAN-Einstellungen**



**Abb. 8b: VLAN-Einstellungen**

Ein zusätzlicher Sicherheitsaspekt ist die Zuweisung eines eigenen VLANs für den internen Management-Port des Switches. Eine Konfiguration des Switches ist dann nur durch den Administrator im entsprechenden VLAN möglich.

Sollte durch eine fehlerhafte VLAN-Konfiguration der Zugang zum Agent blockiert werden, können in solchen Fällen mit der Factory Reset-Funktion sämtliche Einstellungen des Switches zurückgesetzt werden.

## Power-over-Ethernet

Power-over-Ethernet ermöglicht die Stromversorgung von Datenendgeräten, wie IP-Telefonen, Webcams, Access-Points, Zutrittskontrollsystemen usw. über das Twisted Pair Kabel.

Die PoE-Funktion ist im Standard IEEE Std. 802.3af normiert und definiert das Zusammenwirken des Stromversorgers (Power Sourcing Equipment = PSE) und des Stromverbrauchers (Powered Device = PD). Die Stromversorgung wird mit Hilfe einer Steuerspannung zwischen PSE und PD ausgehandelt, wobei mehrere Leistungsstufen unterschieden werden können.

Die Stromversorgung erfolgt nach IEEE 802.3af-Standard auf den nicht belegten Leitungen der RJ45-Buchse (Adern 4 und 5: positiver Anschluss, Adern 7 und 8: negativer Anschluss).

Pro Port können, wie in der Norm definiert, bis zu 15,4 W Leistung an das Endgerät abgegeben werden. Die Speisung erfolgt dabei direkt aus der an dem Switch anliegenden 48V Versorgungsspannung, so dass neben der für den Betrieb des Switches notwendigen Leistung bis zu 4x15,4 W für die angeschlossenen Endgeräte entnommen werden können.

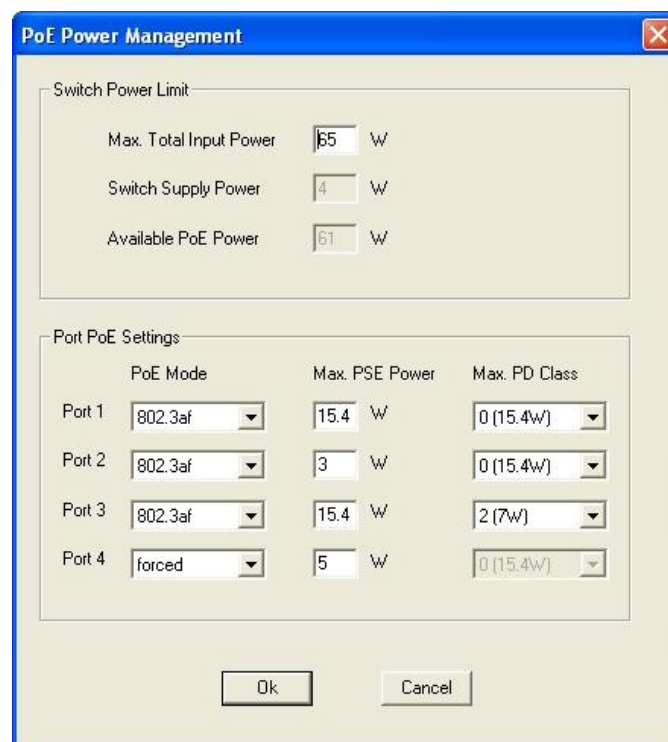
Bei Power-over-Ethernet fähigen Geräten muss diese Funktion aktiviert werden.

Pro PoE-fähigen Anschluss stehen folgende Optionen zur Auswahl:

<i>802.af</i>	Aktivierung gemäß IEEE 802.af, Detection Modus
<i>disabled</i>	Deaktivierung, kein Detection, keine PoE-Funktion
<i>forced</i>	Aktivierung der PoE-Funktion ohne Detection Modus (für nicht IEEE 802.af konforme Geräte)

Max. PSE Power = Limitierung der maximal verfügbaren PoE Leistung

Max. PD Class = Limitierung der anzumeldenden PoE Klassen



**Abb. 9a: Power-over-Ethernet Einstellungen**

The screenshot shows the web management interface for a MICROSENS switch. The browser window title is 'MICROSENS [10.1.1.140] - Mozilla Firefox'. The page title is 'MICROSENS FE Installation Switch - Web Manager'. The interface is in German and shows the following settings:

**Status:** logged in as Admin

**Basic Settings:**

Total Input Power (W)	65
Switch Supply Power (W)	4
Available PoE-Power (W)	61

**Port Settings:**

Port-No.	PoE Mode	PoE Status	permitted Power (W)	measured Power (W)	maximum PD class	detected PD class
Port 1	802.3af	discovering	5	0.0	0 max. 15.4 W	unknown
Port 2	802.3af	discovering	15.4	0.0	2 max. 7.0 W	unknown
Port 3	802.3af	powered	3	1.8	0 max. 15.4 W	0 max. 15.4 W
Port 4	802.3af	discovering	15.4	0.0	0 max. 15.4 W	unknown

Buttons: cancel, apply

**Abb. 9b: Power-over-Ethernet Einstellungen**

Zum Schutz Nicht-PoE-fähiger Endgeräte wird eine Versorgungsspannung erst aufgeschaltet, wenn eine gültige PoE-Signatur des Endgerätes gefunden wurde.

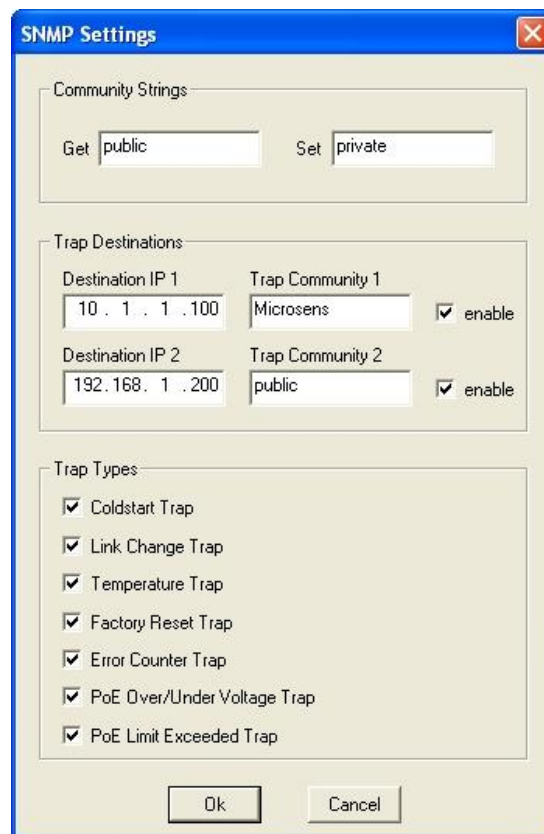
Im aktiven Betrieb wird permanent die entnommene Leistung und die angelegte Spannung überwacht. Werden die zulässigen Grenzwerte über- bzw. unterschritten, wird die Stromversorgung sofort unterbrochen.

## SNMP-Traps

Die Standard Firmware unterstützt SNMP-Traps für die aktive Benachrichtigung von Betriebszuständen.

Folgende Trap-Arten werden unterstützt:

Coldstart Trap	Wird ausgelöst bei Inbetriebnahme des Gerätes bzw. bei Betätigung der Reset-Taste
Link Change Trap	Wird ausgelöst bei Wechsel des Verbindungsstatus am beliebigen Datenanschluss des Gerätes
Temperature Trap	Wird bei Veränderung des Temperatur-Levels ausgelöst
Factory Reset Trap	Wird bei Betätigung beider Reset-Tasten ausgelöst
Error Counter Trap	Wird ausgelöst, wenn ein Error Counter um eine Einheit erhöht wird
PoLAN Over/Under Voltage Trap	Wird ausgelöst, wenn die Ausgangsspannung unter 36 Volt absinkt bzw. 54 V übersteigt (nur bei Geräten mit Power-over-Ethernet Funktion)
PoLAN Limit Exceeded Trap	Wird ausgelöst, wenn die maximal zulässige Leistung erreicht wird. (nur bei Geräten mit Power-over-Ethernet Funktion)



**Abb. 10a: SNMP-Settings**

The screenshot shows the MICROSENS web management interface for an FE Installation Switch. The browser window is Mozilla Firefox, and the URL is http://10.1.1.140/. The page title is "MICROSENS fiber optic solutions FE Installation Switch - Web Manager".

On the left side, there is a navigation menu with the following items: Information, IP-Settings, Port-Settings, Priorization, VLAN-Settings, PoE-Settings (highlighted), MIB, Games, SNMP-Settings, and Admin. The user is logged in as "Admin".

The main content area displays the "Basic Settings" and "Port Settings" sections.

**Basic Settings**

Total Input Power (W)	65
Switch Supply Power (W)	4
Available PoE-Power (W)	61

**Port Settings**

Port-No.	PoE Mode	PoE Status	permitted Power (W)	measured Power (W)	maximum PD class	detected PD class
Port 1	802.3af	discovering	5	0.0	0 max. 15.4 W	unknown
Port 2	802.3af	discovering	15.4	0.0	2 max. 7.0 W	unknown
Port 3	802.3af	powered	3	1.8	0 max. 15.4 W	0 max. 15.4 W
Port 4	802.3af	discovering	15.4	0.0	0 max. 15.4 W	unknown

At the bottom of the Port Settings table, there are "cancel" and "apply" buttons.

**Abb. 10b: SNMP-Settings**

Für die Unterstützung von SNMP-Traps muss mindestens eine IP-Adresse als Zieladresse angegeben werden. Die Device Manager Software unterstützt den Empfang von SNMP-Traps nicht.

Für die Richtigkeit der gemachten Angaben wird keine Haftung übernommen. Aufgrund der ständigen Weiterentwicklung unserer Produkte behalten wir uns technische Änderungen vor. ak/ads2107